

**Technical White Paper** 

## Dell EMC OpenManage Enterprise Login with PingFederate

This technical white paper provides information about configuring OpenManage Enterprise (OME) and PingFederate to enable logging into OME using PingFederate.

#### Abstract

OME 3.5 provides a method to log in using OpenID Connect (OIDC) providers—PingFederate. OIDC providers are the identity and user management software that allow users to securely access applications.

November 2020

#### Revisions

Date	Description
Nov 2020	Initial release

## Acknowledgements

Author: Venkata Donepudi, Balaji Shanmugam and Manish Agrawal

The information in this publication is provided "as is." Dell Inc. makes no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose.

Use, copying, and distribution of any software described in this publication requires an applicable software license.

Copyright © November 2020 Dell Inc. or its subsidiaries. All Rights Reserved. Dell Technologies, Dell, EMC, Dell EMC and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners. [11-Nov-20] [Technical White Paper] [Dell EMC OpenManage Enterprise Login with PingFederate | 454]

## Table of contents

Re	vision	۱۶	2
Acl	knowl	ledgements	2
Tal	ole of	contents	3
Exe	ecutiv	ve summary	4
1	Syst	tem Requirements & Prerequisites	5
2	OME	E and PingFederate Configurations	6
	2.1	Configure Scope and Policy in PingFederate	6
	2.2	Configure Time in PingFederate and OME	9
	2.2.2	1 PingFederate time configuration	9
	2.2.2	2 OME time configuration	9
	2.3	Enable Dynamic Client registration in Ping Federate	10
3	Ope	nID Connect Provider Registration in OME	11
	3.1	Register an OpenID Connect Provider with Username and Password in OME	11
	3.2	Register an OpenID Connect Provider with Initial Access Token in OME	11
4	Con	figure OAuth Client for dxcua scope and signing algorithms in PingFederate	14
5	Logi	in from OME using PingFederate Users	15
6	Gen	eral Troubleshooting of Issues	
Α	Rela	ated resources	19

#### **Executive summary**

In this white paper, you will learn how to configure PingFederate and OpenManage Enterprise (OME) or OpenManage Enterprise-Modular (OME-M) to enable you to log into OME using PingFederate.

Integrating OME with PingFederate allows PingFederate users (Users associated to data store in PingFederate) to log into OME.

After OME is integrated with PingFederate, user authentication in OME will be delegated to PingFederate.

## 1 System Requirements & Prerequisites

The following are the system requirements:

- PingFederate version 10.1
- OpenManage Enterprise version 3.5 or later

The following are the prerequisites before integration of OME with PingFederate:

- User has prior knowledge of:
  - PingFederate
  - OpenManage Enterprise
  - OpenID Connect specifications
- > PingFederate is installed and configured with:
  - LDAP or External Data Source
  - Access Token Management
  - Identity Provider Configuration
  - Policies and Grant Mappings
  - All prerequisites for Dynamic client registration

If these prerequisites are not met, see the PingFederate help guide(<u>https://docs.pingidentity.com/bundle/pingfederate-101/page/qem1584122852896.html</u>) for fulfilling the prerequisites.

## 2 OME and PingFederate Configurations

This section describes the configuration required to enable user authentication in PingFederate.

#### 2.1 Configure Scope and Policy in PingFederate

To enable OpenManage Enterprise OpenID Connect login using PingFederate, you must add and map a scope dxcua to the Client ID and define the user privileges. The Dell Extended Claim for User Authentication (dxcua) is necessary to identify the user roles and permissions required to manage OME.

To configure dxcua claim in PingFederate, do the following:

- 1. Log into PingFederate with administrative privileges.
- 2. Navigate to System->OAuth Settings->Scope Management->Exclusive Scopes
- 3. Set Scope Value to dxcua and Scope Description to Dell Extended Claim for User Authentication as shown below in Figure 1.

Ping	Federate			AUTHENTICATION	APPLICATIONS	SECURITY	SYSTEM				Q	0	٩
	< OAuth Settings	Scope Management											
007	Authorization Server Settings	Common Scopes Exclusive	e Scopes Default Scope										
	Scope	Exclusive scopes aren't available to	OAuth clients by default unless individual clients a	are configured to allow (	exclusive scopes. Scop	pes can be declared	l as dynamic, wh	ich allows OAuth clients to request scopes v	where a compone	ent of the scope n	ame is variable.		
۲	Management	Scope Value	Scope Description			Dynamic Actio	n						
~	Client Settings	dxcua	Dell extended claim for user authentication			Edit I	Delete						
$\sim$	Client	DynamicClientRegistration	DynamicClientRegistration			Edit I	Delete						
ţ.	Registrations Policies					Ad	bd						
<>													
		Scope Group Value	Scope Group Description			Sub Scopes		Action					
						DynamicCl dxcua	ientRegistration	Add					
									Cancel	Previous	Next	Save	

Figure 1 – PingFederate: Scope Management

After defining the dxcua scope, it is required to map dxcua to the PingFederate Policy.

To map "dxcua" scope to PingFederate Policy, do the following:

- 1. Navigate to Applications -> OpenID Connect Policy Management-> Select Policy-> Manage Policy tab.
- 2. Select the INCLUDE USER INFO IN ID TOKEN check box as shown in Figure 2.

Ping	Federaté		Authentication <u>applications</u> security system	Q   @   ®
	< OAuth	OpenID Connect Policy Mana	ement   Policy	
Ð	Clients	Manage Policy Attribute Contract	Attribute Scopes Attribute Sources & User Lookup Contract Fulfillment Issuance Criteria Summary	
Ð	Access Token Management	Enter a Policy ID and Name. You may also char	e general settings for the ID Token.	
ψ	Annual Victoria	POLICY ID	OMEPolicy	
	Access Token Mappings	NAME	OMEPolicy	
	OpenID Connect Policy Management	ACCESS TOKEN MANAGER	OMEAccessToken v	
	CIBA Request	ID TOKEN LIFETIME	20 minutes	
		INCLUDE SESSION IDENTIFIER IN ID TOKEN		
		INCLUDE USER INFO IN ID TOKEN	V	
		INCLUDE STATE HASH IN ID TOKEN		
		RETURN ID TOKEN ON REFRESH GRANT		
		Manage Access Token Managers		
			c	ancel Next Save

Figure 2 - PingFederate: OpenID Connect Policy Management -> Manage Policy

3. Navigate to Attribute Scopes tab and add the dxcua scope attribute as shown in Figure 3.

Ping	Federate		AUTHENTICATION	APPLICATIONS SECURITY SYSTEM	м	오   ⑦
	< OAuth	OpenID Connect Policy Man	agement   Policy			
2	Clients	Manage Policy Attribute Contract	Attribute Scopes Attribute Sources & User Lookup	Contract Fulfillment Issuance Criteria	Summary	
٨	Access Token Management	Scopes are used in OpenID Connect to cont	trol the attributes that are released to OAuth clients. On this pa	ge you may add associations between scopes and at	tributes beyond what is defined in the specification.	
ŵ	Access Token Mappings					
		Scope	Attributes	Action		
	OpenID Connect	dxcua	dxcua	Edit I Delete		
	Management CIBA Request	- SELECT - 🗸		Add		
	Policies				Can	ncel Previous Next Save

Figure 3 – PingFederate: OpenID Connect Policy Management -> Attribute Scopes

- 4. Navigate to Contract Fulfilment and:
  - a. Select **Text** as a source for the **dxcua** scope.
  - b. Add [{"Role": "CA,AD"}] for enabling administrator privileges in OME as shown in Figure 4.

<b>Ping</b> Federate			Althentication <u>Applications</u> security system	୍ । ଡ   ଏ
APPLICATIONS	OpenID Connect Polic	cy Management   Policy		
Integration	Manage Policy Attribute C	Contract Attribute Scopes Attribute Source	es & User Lookup Contract Fulfillment Issuance Criteria Summa	ny l
🔊 OAuth 🔉	Fulfill the Attribute Contract with va	alues from the Access Token or from other sources li	sted.	
💱 Token Exchange	Attribute Contract	Source	Value	Actions
	address.country	No Mapping V		None available
	address.formatted	No Mapping V		None available
	address.locality	No Mapping V		None available
	address.postal_code	No Mapping ~		None available
	address.region	No Mapping ~		None available
	address.street_address	No Mapping V		None available
	birthdate	No Mapping ~		None available
	dxcua	Text ~	[("Role": "CA.AD"]]	None available
	email	No Mapping V		None available

Figure 4 – PingFederate: OpenID Connect Policy Management -> Contract Fulfillment

The configuration in step-4 allows OAuth clients using the policy selected in step-4 to login users into OME with administrator privileges. OME supports other roles along with the administrator role.

The following are the dxcua roles available in OME. See the OME User's Guide for more information about each user role.

Role	Abbreviation
Administrator	AD
Device Manager	DM
Viewer	VE

The following are the dxcua roles available in OME-M. See the OME-M User's Guide for more information about each user role.

Role	Abbreviation
Chassis Administrator	CA
Computer Manager	СМ
Fabric Manager	FM
Storage Manager	SM
Viewer	VE

#### 2.2 Configure Time in PingFederate and OME

It is required that both OME and PingFederate should reflect the same time to avoid issues in validating Authorization Code, Access Token, and User ID token. Ensure that OME and PingFederate are pointing to the same time source.

#### 2.2.1 PingFederate time configuration

See the PingFederate help guide (<u>https://docs.pingidentity.com/bundle/pingfederate-101/page/qem1584122852896.html</u>) to sync time from Host Operating System.

#### 2.2.2 OME time configuration

To configure time in OME, do the following:

- 1. Log into OME with administrative privileges.
- Navigate to Application Settings ->Network -> Time Configuration and configure time either by selecting Use NTP or configure Time and Time Zone as shown in Figure 5.

DpenManage Enterprise	OpenManage Enterprise							
🛉 Home 🗏 Devices 🔅 Configuration 🗸 🚩 Alerts 🗸 🛽	⊠Monitor 🗸 🔹 ♦ Application Settings 🗸						2	×
Application Settings								
Network Users Licenses Console Preferences St	ecurity Alerts Incoming Alerts Warranty Console and Plugins Script Execution Mobile							
<ul> <li>Current Settings</li> <li>Session Inactivity Timeout Configuration</li> <li>Time Configuration</li> </ul>								
Timezone	(GMT+00:00) Coordinated Universal Time							
Use NTP	0							
Primary NTP Server Address	dell.ntp.primary.com							
Secondary NTP Server Address	dell.ntp.secondary.com							
Tertiary NTP Server Address								
System Time	Oct 29, 2020 6:19:53 PM							
Time Source	Local Clock							
Apply Discard								

Figure 5 - OME: Time Configuration

#### 2.3 Enable Dynamic Client registration in Ping Federate

Dynamic Client Registration allows OME to register clients on PingFederate via APIs either by using username and password or Initial Access Token. By default, Dynamic Client registration is disabled on PingFederate and is enabled only when external data sources such as an external database or AD/LDAP is configured in PingFederate.

To enable Dynamic Client Registration, do the following:

- 1. Log into PingFederate as an admin user.
- 2. Navigate to System-> OAuth Settings -> Client Settings -> Dynamic Client Registration.
- 3. Select all the check boxes of the fields as shown in Figure 6.
- Select any existing scope for INITIAL ACCESS TOKEN SCOPE or create a new scope called DynamicClientRegistration scope similar to configuring dxcua in Configuration of Scope in PingFederate section.

Ping	Federate			АЛТНЕ	NTICATION APPLICATIONS	SECURITY	SYSTEM			Q	0
	< OAuth Settings	Client Settings									
00	Authorization Server Settings	Dynamic Client Registration	Scope Constraints	Client Configuration Defaults	Client Registration Policies						
蒜	Scope Management	Allow developers to register OAuth o management and choose to rotate th	clients via an API in a st he registration access t	tandardized way and optionally ma token or the client secret on each r	nage them. You can enable or disa nanagement call as well allowing o	ble dynamic client lient deletion.	registration and choose whether reg	istration requires an access token. Also,	, you can enable or disat	ole dynamic cli	ent
8	Client Settings	ENABLE DYNAMIC CLIENT REGISTI	RATION								
×	Client	REQUIRE INITIAL ACCESS TOKEN	\$								
Ą	Registrations Policies	INITIAL ACCESS TOKEN SCOPE	Dyna	micClientRegistration 🗸							
<> P	otocol Metadata	ENABLE DYNAMIC CLIENT REGISTI MANAGEMENT	RATION								
		ROTATE CLIENT SECRET	~								
		ROTATE REGISTRATION ACCESS T	OKEN 🖌								
		ALLOW CLIENT DELETE	~								
									Cancel	hiert	Save
									Gander	HEAL	

Figure 6 - PingFederate: Client Settings

It is recommended to select **ROTATE CLIENT SECRET** and **ROTATE REGISTRATION ACCESS TOKEN** which will change Client Secret and Registration Access Token when modifying or querying client registration.

PingFederate will not allow Dynamic OAuth client registration using both username and password and Initial Access Token at the same time. Disable **REQUIRE INITIAL ACCESS TOKEN** for username and password-based OAuth client registration to be successful. When **Require Initial access token** is enabled, only access token will work for registration.

## 3 OpenID Connect Provider Registration in OME

When you register an OpenID Connect provider in OME using username and password or Initial Access Token, it generates an OAuth client in PingFederate.

## 3.1 Register an OpenID Connect Provider with Username and Password in OME

To register OpenID, Connect Provider with username and password, do the following:

- 1. Log into OME with administrative privileges.
- 2. Navigate to Application Settings -> Users -> OpenID Connect Providers -> Add.
- 3. Enter information in the required fields as shown in Figure 7.

DpenManage Enterprise			Search Everything	Q	<b>G</b> 15 Pro	🛓 admin	
🕈 Home 📕 Devices 🗇 Configuration 🗸 🌾 Alerts 🗸 🖂 Monitor	Add New OpenID Connect Provid Fill out the information below to ad	ier d a new OpenID Connect provider.	0 X				×
C Application Settings							
Network Users Licenses Console Preferences Security	Name	Test-OIDC					
	Discovery URI 🌗	https://pingfederate101.smd.devops.dell.com	]				
Users User Sessions Directory Serv	Authentication Type	Usemame	]				
444 Frabla Disabla Dalata	Username	admin	]				
	Password		]	PERINTPA	TION STATUS		
	Certificate Validation	0					
0 item(s) found, 0 item(s) selected. Displaying items 0 - 0.	Test connection	Test URI and SSL Connection					
	Enabled 🚺	2					
		F	Finish Cancel				

Figure 7 - OME: Add New OpenID Connect Provider using username and password

The user (local PingFederate User or AD/LDAP User in PingFederate) information used to register OpenID Connect Provider should have proper privileges to create OAuth client in PingFederate.

# 3.2 Register an OpenID Connect Provider with Initial Access Token in OME

To register OpenID, Connect Provider with Initial Access Token, do the following:

- 1. Log into OME with administrative privileges.
- 2. Navigate to Application Settings -> Users -> OpenID Connect Providers -> Add.
- 3. Enter information in the required fields as shown in Figure 8.

🔛 OpenManage Enterprise			Search Everything
🐂 Home 🔳 Devices 🔅 Configuration 🗸 💌 Alerts 🗸 🖼 Monitor	Add New OpenID Connect Prov Fill out the information below to a	rider dd a new OpenID Connect provider.	Θ×
C Application Settings			
Network USERS Licenses Console Preferences Security	Name	Test-OIDC	
	Discovery URI 🕕	https://pingfederate101.smd.devops.dell.com	
Users User Sessions Directory Serv	Authentication Type	Initial Access Token 🗸	
Add Enable Disable Delete	Initial Access Token	TfVQ0dy4wPmHix_LA-QF ZDGvFRY0NnYE0pFNN4WhvyIXeJLVriwVxj6itbcK00B0E61vW3_A1cD li1pL_qrJFa_9W2cKCrm1Skw_V3fdKbioHpYuYFFuQ2Ubr9N0vuLPcAW	
		NTIK0Ja01ai5L9fVrpA	
0 item(s) found, 0 item(s) selected. Displaying items 0 - 0.	Certificate Validation		
	Test connection	Test URI and SSL Connection	
	Enabled 🕕		
		Fir	nish Cancel

Figure 8 - OME: Add New OpenID Connect Provider using Initial Access Token

To get the Initial Access Token, see the guidelines mentioned in the PingFederate help guide (<u>https://docs.pingidentity.com/bundle/pingfederate-101/page/qem1584122852896.html</u>)

For example: Create an OAuth Client in PingFederate and use that OAuth client to provide the Access Token.

The following are the sample request and response for getting initial access token using IMPLICIT flow.

#### **Request for Initial Access token:**

curl --location --request POST

/as/authorization.oauth2?client\_id=DynamicClientRegistration&response\_type=token&redirect\_uri=https://<callback url>&scope=DynamicClientRegistration' \

--header 'Authorization: Basic dGVzdDp0ZXN0'

#### Successful Response:

302

https://XXXX #access\_token=

eyJhbGciOiJSUzI1NiIsImtpZCl6IkExOjMwOjIzOjUzOjVEOkJCOjE5OjU3IiwicGkuYXRtIjoieG1wdiJ9.eyJzY29wZSl6IkR5b mFtaWNDbGIIbnRSZWdpc3RyYXRpb24iLCJjbGIIbnRfaWQiOiJEeW5hb &token\_type=Bearer&expires\_in=7199 On successful registration of OpenID Connect provider in OME, the OIDC is displayed as shown in Figure 9.

OpenManage Enterprise											
🕈 Home	🗏 Devices	s 🦻 🍄 Config	uration 🗸	🚩 Alerts 🗸	🔤 Monitor	🗸 🗘 🗘 A	pplication Settings 🗸				
🌣 Appl	lication	Settings	5								
Network	Users	Licenses	Console P	references	Security	Alerts	Incoming Alerts	Warranty	Consol	e and Plugins	Script Execution
	Users	Use	rSessions		Directory Ser	rvices	OpenID Co	nnect Provider	s		
Add	Enable	Disabl	e De	lete							
NAM	E				EN	ABLED	DISCOVERY UR	1			
Test-OIDC		[~	']	https://pingfe	https://pingfederate101.smd.devops.dell.com						

Figure 9 - OME: Successful Registration

#### Notes:

- Discovery URI specified in OIDC configuration wizard should have valid endpoint of the provider listed.
- Test connection in configuration wizard is anonymous, the credentials or Initial access token specified is used for registration.
- When cert is used in OIDC configuration, the Name of OIDC provider mentioned in Discovery URI should match the OIDC providers Issuer endpoint name and the OIDC Providers SSL Certs "Subject CN" or "Subject alternative name" for OIDC login to work.
- OME supports only ClientID and Secret based client authentication.
- Maximum of 4 OIDC providers can only be used with OME.
- Test Registration status button is available to test the registration status of an OIDC configuration.

# 4 Configure OAuth Client for dxcua scope and signing algorithms in PingFederate

After OpenID Connect provider is registered in OME successfully, a new OAuth client is created in PingFederate. Dynamically registered OAuth client shall be configured to use the dxcua scope and OME compatible signing algorithm for ID Token.

To configure dxcua scope and signing algorithm, do the following:

- 1. Log into PingFederate with administrative privileges.
- Navigate to Applications -> OAuth Clients -> Select Client and configure Exclusive Scopes and ID Token Signing Algorithm as shown in Figure 10.

EXCLUSIVE SCOPES	<ul> <li>Allow Exclusive Scopes</li> </ul>			
	✓ dxcua			
OPENID CONNECT	ID Token Signing Algorithm			
	RSA using SHA-256	~		

Figure 10 - PingFederate: configuring Exclusive Scopes and ID Token Signing Algorithm in OAuth Client.

#### 5 Login from OME using PingFederate Users

OME displays successfully registered OpenID Connect Providers on the login page. Users can choose to log into OME with username and password credentials of users local to OME or with any one of the registered OpenID Connect Providers.

To log into OME with PingFederate Users, do the following:

- 1. Navigate to the OME login page.
- 2. OME login page displays successfully registered OpenID Connect Provider(s) as shown in Figure 11.

Oper	EEEECC	erprise	
User Name Password Login	OR	Log in with Test-OIDC	

Figure 5 - OME: Login Screen

#### 3. Select Login with OpenID Connect Provider Name.

The browser is redirected to PingFederate website and challenge the user for credentials. If basic auth is enabled in PingFederate then following screen is displayed. Else the PingFederate admin console page is displayed.

Sign in https://pingfe	ederate101.smd.devops.dell.com	
Username		
Password		
	Sign in	Cancel

Figure 12 – PingFederate: Credentials Screen

After validating the credentials successfully, if user consent setting is enabled in PingFederate then user will be prompted to provide access permissions as shown in Figure 13.

Request for Approval						
	Logged in as <b>omeuser</b>					
PingFederate is requesting permission for the following:         Image: ACCESS TO YOUR USERNAME         Image: Sign in with openid connect         Image: Dell extended claim for user authentication	Client : PingFederate					
Allow Don't Allow						

Figure 13 - PingFederate: Consent Screen

After providing the necessary permissions, the browser is redirected to OME and the user will be logged into OME based on the response from PingFederate.

After successful login to OME, information about the user is displayed in the upper right corner as shown in Figure 14.



Figure 14 - OME: Successful Login

#### 6 General Troubleshooting of Issues

1. If you see the error 'Unable to log in by using the Graphical User Interface (GUI) because Insufficient privileges' while logging into OME then ensure that dxcua claim is added in Ping Federate Server.

OpenManage Enterprise						
	D≪LLEMC					
🔇 Unable to log in b	by using the Graphical User Interface (GUI) because Insufficier	t privileges to perform the operation .				
User Name Password		Log in with Test ODC				
Login	OR Da					

2. If you see the error 'Unable to log in by using the Graphical User Interface (GUI) because OIDC server time is different from System time' while logging into OME then ensure that OME and PingFederate Server are in the same time zone.

EEEEE OpenManage Enterprise							
	D∕¢LLEMC						
Unable to log in by using the second seco	e Graphical User Interface (GUI) because OIDC	server time is diffe	erent from System time				
User Name Password Login	OR	\;	Log in with Test-ODC				

3. For any other issues see the PingFederate Server log.

Dell EMC OpenManage Enterprise Login with PingFederate

## A Related resources

Dell EMC OpenManage Enterprise documents